

Seamless Transition: Mastering Migration to Cisco Secure Firewall

cisco Live !

Raghunath Kulkarni
Principal Engineer – Security TAC

Foster Lipkey
Principal Engineer – Security TAC

Cisco Webex App

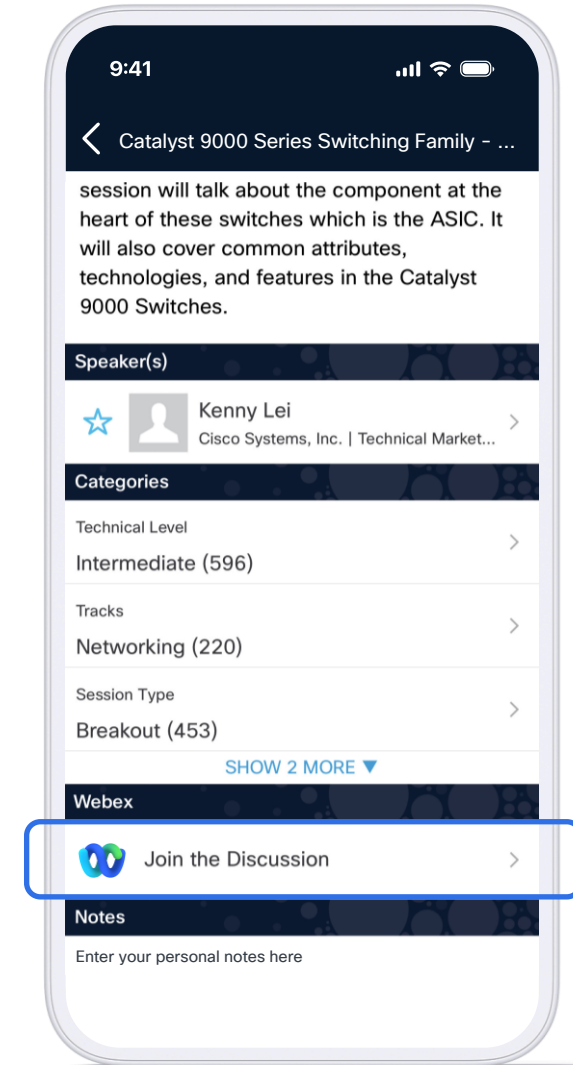
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2058>

Agenda

- 01 Migration Lifecycle
- 02 Getting Started
- 03 Firepower Migration Tool
- 04 Firepower Device Migration
- 05 Bonus Content: Firepower Management Center Model Migration
- 06 References

Your Speaker(s)



Raghunath Kulkarni

Principal Engineer – Security TAC

- 15+ Years of Security Experience
- PIX -> ASA -> FWSM/ASA-SM -> Sourcefire ->FTD
- Sourcefire Veteran
- 2 Defensive Publications (UEBA & IoT Trust)
- 2 Cisco Patents (AI Identity & SecOps)
- Cisco Press Author in making



Foster Lipkey

Principal Engineer – Security TAC

- 13+ Years of Security Experience
- Cisco Live Distinguished Speaker
- Snort Expert
- Sourcefire Veteran
- Automation Enthusiast
- 1 – Malware Detection Patent Holder

Before We Begin Pact



It won't be a step by step
configuration guide...

Download the PDF
version of this deck-
there is a ton of
reference slides.



All slides = Death
by PowerPoint...

Before We Begin Pact

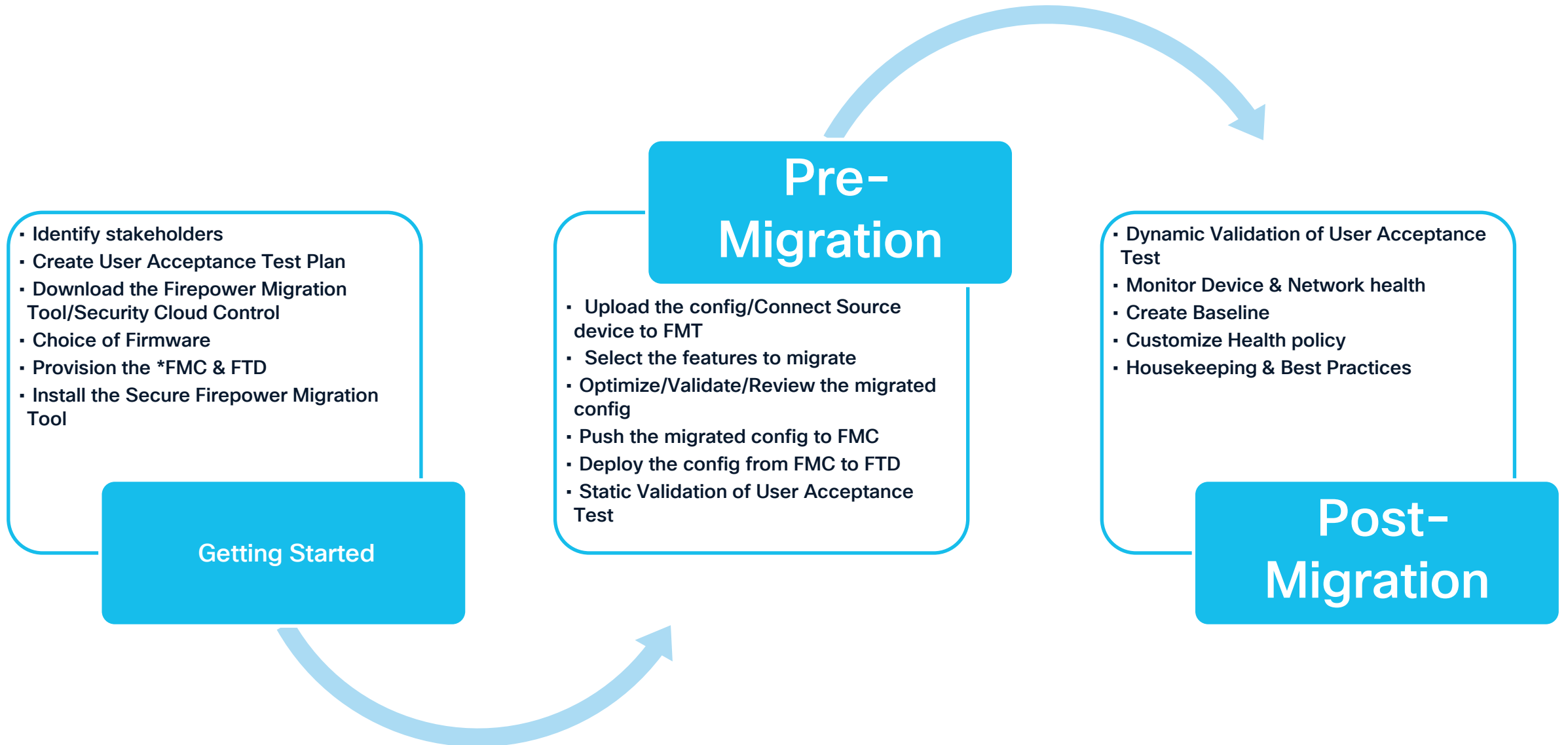
The content of this deck improves and evolves
with your valuable feedback!



Put your email in the comment – I WILL respond 😊

Migration Lifecycle

Migration Workflow



Getting Started

Behind the Scenes

01

Identify
Stakeholders

02

Installation
(FMC,FTD &
FMT)

03

Software
Conformance

04

Version
Compatibility

05

Features
Available

06

User
Acceptance
Test

Firepower Migration Tool

Firepower Migration Tool



Air gapped version available on demand



System & File Permissions



Pop-Up Blockers (Authentication in browser)



Always run the latest version of Firepower Migration Tool (Uninstall any older versions)

Pre-Migration Phase

FMT Navigation

 Firewall Migration Tool (Version 7.7)

Select Source Configuration

Source Firewall Vendor

Select Source ^

Cisco Legacy Firewalls

Cisco ASA (8.4+)

Cisco ASA (9.2.2+) with FirePOWER Services

Cisco Secure Firewall Device Manager (7.2+)

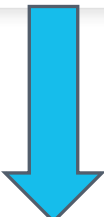
Third Party Firewalls

Check Point (r75-r77)

Check Point (r80-r81)

Fortinet (5.0+)

Palo Alto Networks (8.0+)



Source Device Selector

Cisco ASA (8.4+) Pre-Migration Instructions

 This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) when migration is in progress.

Session Telemetry:

Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:

FMT: Firewall Migration Tool	FMC: Firewall Management Center
FTD: Firewall Threat Defense	

Before you begin your Adaptive Security Appliance (ASA) to Firewall Threat Defense migration, you must have the following items:

- **Stable IP Connection:**
Ensure that the connection is stable between FMT and FMC.
- **FMC Version:**
Ensure that the FMC version is 6.2.3 or later. For optimal migration time, improved software quality and stability, use the suggested release for your [FTD](#) and [FMC](#). Refer to the gold star on CCO for the suggested release.
- **FMC Account:**
Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration.
- **FTD (Optional):**
To migrate the device configurations like interfaces, routes, and so on, add the target device to FMC. Skip this step if you want to migrate only the shared configurations like objects, NAT, ACL, and so on.



The console must stay open while the Secure Firewall Migration Tool is open and running

FMT Navigation

Select Source Configuration ⓘ

Source Firewall Vendor

Check Point (r75-r77) ▼

Start Migration

Demo Mode

Check Point (r75-r77) Pre-Migration Instructions



This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) when migration is in progress.

Session Telemetry:

Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:

FMT: Firewall Migration Tool

FMC: Firewall Management Center

FTD: Firewall Threat Defense

Before you begin your Check Point (CP) to Firewall Threat Defense migration, you must have the following items:

- **Stable IP Connection:**

Ensure that the connection is stable between FMT and FMC.

- **FMC Version:**

Ensure that the FMC version is 6.2.3 or later. For optimal migration time, improved software quality and stability, use the suggested release for your FTD and FMC. Refer to the gold star on CCO for the suggested release.

- **FMC Account:**

Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration.

- **FTD (Optional):**

To migrate the device configurations like interfaces, routes, and so on, add the target device to FMC. Skip this step if you want to migrate only the shared configurations like objects, NAT, ACL, and so on.

- **Check Point Configuration Requirements:**

Export Configuration file from Check Point to a zipped file using Web Visualization Tool and Python script, which contains the following files: communities.xml, index.xml, NAT_Policy.xml, network_objects.xml, Security_Policy.xml, Services.xml and networking.txt

To migrate following features in Check Point

- **Remote Deployment:** For FMC and FTD version 6.7 or later, if the Remote Deployment is enabled, the Firewall Migration Tool will only migrate ACLs, Network Objects, Port Objects, and NAT. You must migrate the Interfaces and Route configurations manually on the FMC.

- **Interface Requirements:**

- If the source Check Point firewall gateway contains configurations for port channel interfaces, then pre-configure the port channel interfaces in FMC for the Container based FTD.

- Migration to FTD with Cluster interface configuration is not supported. Remove the existing cluster interface configuration before using the device as the Target FTD. Alternatively, you can choose to proceed with 'No FTD Flow' in the Select Feature page where or in which case "Interfaces & Routes" will not be migrated .

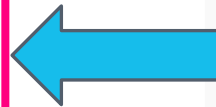
- **Power Options:**

Ensure that your system does not enter the sleep mode during a large migration push.

- **Default Browser:**

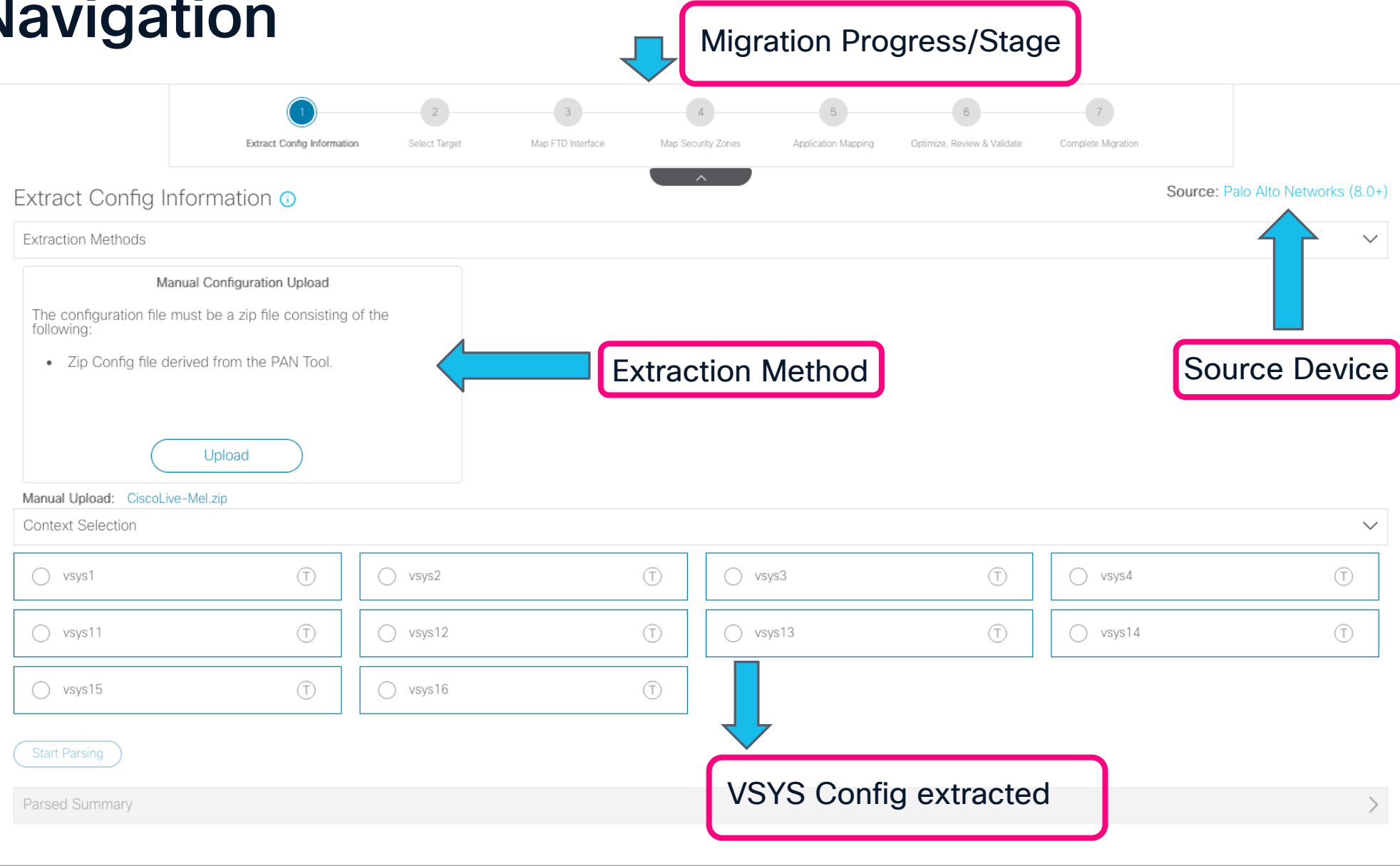
Google Chrome or Microsoft Edge.

Guidelines & Instructions
specific to the source firewall
vendor selected

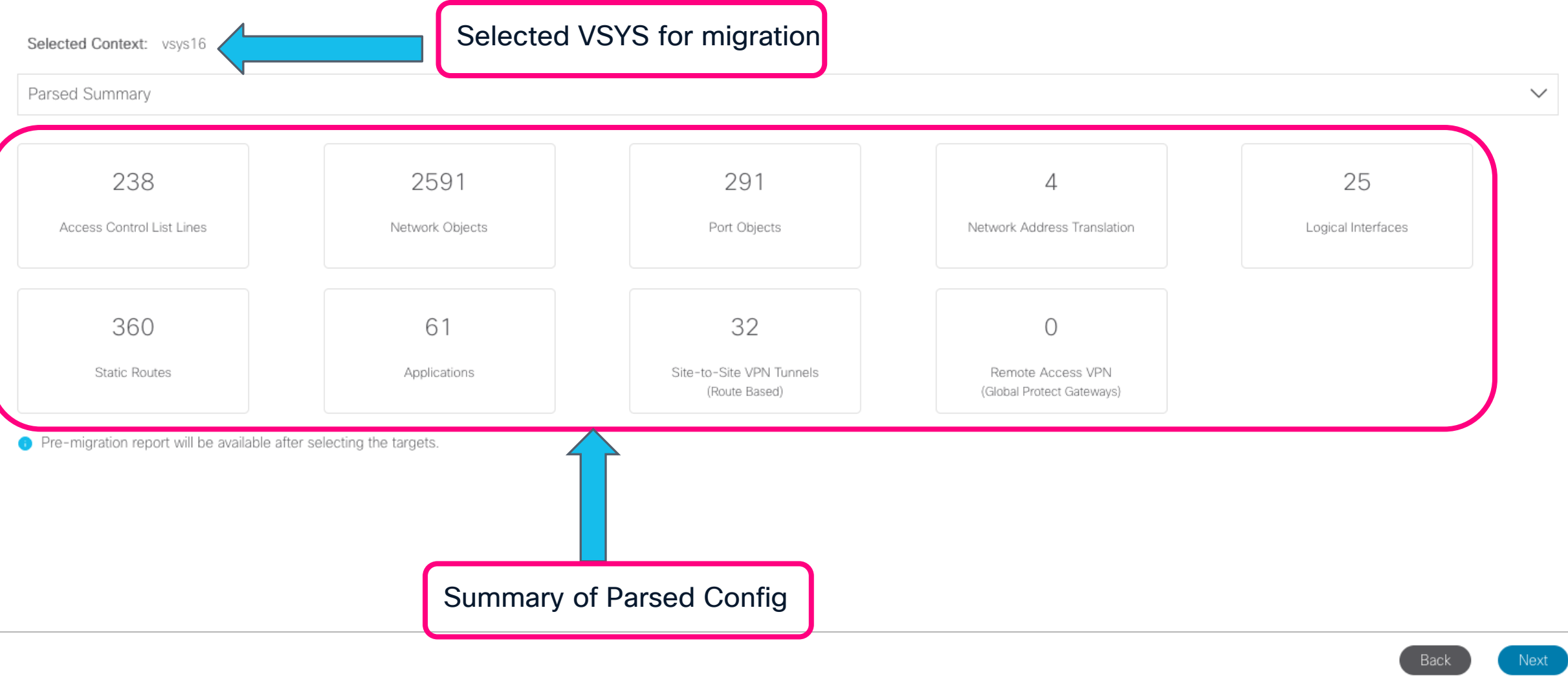


Ensure the right config extraction methods are used based on source device

FMT Navigation



FMT Navigation



Pre-Migration Report

Overall Summary

- Summary of the config that is successfully migrated.
- Policy names, Rule counts, Objects, Logical interfaces, Applications, Static routes, VPN config etc.

Config lines with errors

- Information about configuration elements that couldn't be migrated successfully due to parsing issues by the FMT
- Network Objects, Routes etc. (Fix them and re-upload the config file from source device)

Ignored configurations

- List of all the configuration elements that are ignored by FMT during migration
- Review these lines, verify whether each feature is supported in FMC



Pre-Migration report provides insights into corrective actions if there are any errors identified in config

Target Selection

Migration Progress/Stage

Choice of FMC

Firewall Migration Tool (Version 7.7)

1

2

3

4

5

6

7

Extract Config Information

Select Target

Map FTD Interface

Map Security Zones

Application Mapping

Optimize, Review & Validate

Complete Migration

Source: Palo Alto Networks (8.0+)

Firewall Management

On-Prem FMC (Hardware/Virtual)

Cloud-delivered

FMC IP Address/Hostname/FQDN

10.197.241.164

Connect

Choose FTD

Select Features

Rule Conversion/ Process Config

FMC Login

IP Address/Hostname/FQDN

10.197.241.164

Username

fmt_user

Password

.....

Login

Target Selection

 Firewall Migration Tool (Version 7.7)

1

2

3

4

5

6

7

Extract Config Information

Select Target

Map FTD Interface

Map Security Zones

Application Mapping

Optimize, Review & Validate

Complete Migration

7

?

⚙

🔄

Select Target ⓘ

Source: Palo Alto Networks (8.0+)

Firewall Management

FMC IP Address/Hostname/FQDN: 10.197.241.164

Choose FTD

☒ Select FTD Device

Select FTD Device

Standalone FTD

10.197.241.96 (10.197.241.96) - VMWare (Native) (R)

10.197.239.26 (10.197.239.26) - VMWare (Native) (R)

HA-Pairs

migration-HA

☐ Proceed without FTD

Option to proceed without FTD

List of registered devices on FMC

Feature Selection

 Firewall Migration Tool (Version 7.7)

1 Extract Config Information 2 **Select Target** 3 Map FTD Interface 4 Map Security Zones 5 Application Mapping 6 Optimize, Review & Validate 7 Complete Migration

Select Target ⓘ Source: [Palo Alto Networks \(8.0+\)](#)

Firewall Management >

FMC IP Address/Hostname/FQDN: 10.197.241.164

Choose FTD >

Selected FTD: 10.197.241.96

Available Features for migration

Select Features ▾

Device Configuration	Shared Configuration	Advanced Configuration
☒ Interfaces	☒ Access Control	Optimization ★
☒ Routes	☐ Migrate policies with Application-default as Enabled ⓘ	☒ Migrate Only Referenced Objects
☒ Site-to-Site VPN Tunnels	☒ Network Objects	Access Control Options
☐ Policy Based (Unsupported) ⓘ	☒ Port Objects	☒ Select AD/LDAP Realm ⓘ
☒ Route Based (VTI)	☐ Remote Access VPN	Discovered Identities
<button>Proceed</button>		Special Identities

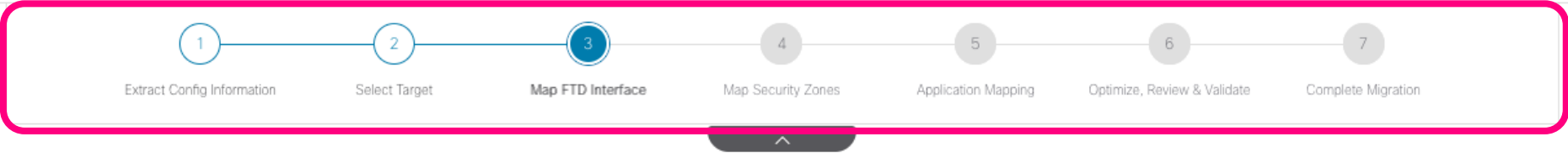
Rule Conversion/ Process Config >



Enable this to ensure that unused objects are not migrated and only referenced one are migrated

Interface Mapping

Migration Progress/Stage



Map FTD Interface ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: FTD-2-Instance-1

PAN Interface Name	FTD Interface Name	Mapped Nameif
ae1	Port-channel1 ▾	ae1
ae2		
ae2.3204	Ethernet1/1.10 ▾	ae2_3204
ae2.3205	Ethernet1/1.100 ▾	ae2_3205
ae3	Ethernet1/2 ▾	ae3
ae3.3200	Ethernet1/1.20 ▾	
ae3.3201	Ethernet1/1.30 ▾	ae3_3201
ae3.3202	Ethernet1/1.40 ▾	ae3_3202
ae3.3203	Ethernet1/1.50 ▾	ae3_3203
ae3.3299	Ethernet1/1.60 ▾	ae3_3299

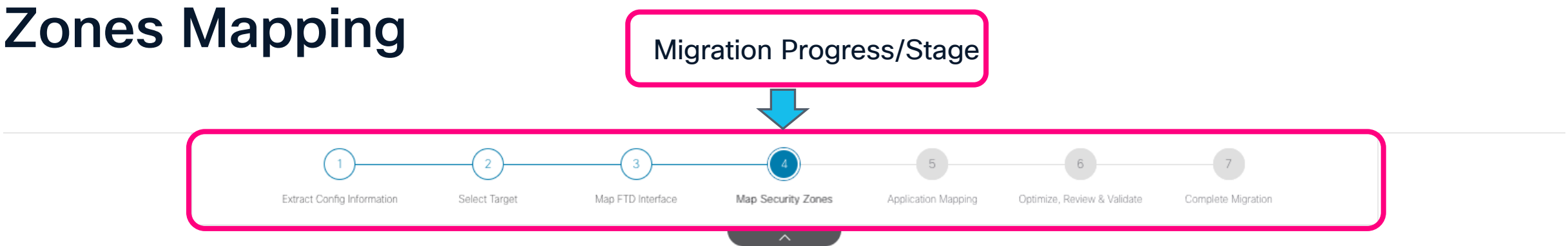
Source Device Interface List

FTD Device Interface List



Ensure that number of interfaces on FTD is greater than or equal to Source Device interface

Zones Mapping



Map Security Zones ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: FTD-2-Instance-1

Add SZ

Auto-Create

PAN Zone Name	FMC Security Zones
<input type="text"/>	
Inside	Select Security Zone
Outside	Select Security Zone
DMZ	Select Security Zone
VPN	Select Security Zone
Prod	Select Security Zone
Staging	Select Security Zone
Servers	Select Security Zone
Guest	Select Security Zone

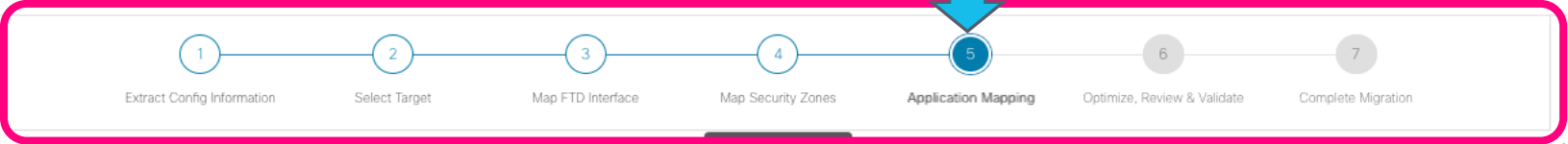
This would auto-create zones identical to Source Device Zones

Manual zone creation

Note: Interfaces that are used in multiple configurations are allowed to have their unique security zones. The security zone mapping section for these interfaces will be greyed out.

Application Mapping (1/2)

Migration Progress/Stage



Application Mapping ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: FTD-2-Instance-1

✔ Valid Mappings (37/42) ⚠ Blank Mappings (5/42) ✖ Invalid Mappings (0/42)

Valid Source Applications	Mapping Mode	Target Application/Ports
<input type="text"/>		
ms-netlogon	application	Netlogon
msrpc	application	DCE/RPC
rpc	application	ERPC
snmp-trap	application	SNMP trap (Deprecated)
windows-remote-management	application	Microsoft WSMAN
tracert	application	tracert (Deprecated)
vmware	application	VMware vCenter client,VMware Fault Domain Manager, VMWare Remote Authentication, VMware Horizon View, VMware Server Console
ssl	application	SSL
active-directory	application	AD DSAOP
dns	application	DNS

↑

Auto Mapping of Applications

Application Mapping (2/2)

Migration Progress/Stage

1

2

3

4

5

6

7

Extract Config Information

Select Target

Map FTD Interface

Map Security Zones

Application Mapping

Optimize, Review & Validate

Complete Migration

Application Mapping ⓘ

Source: Palo Alto Networks (8.0+)

Target FTD: FTD-2-Instance-1

Clear Mapped Data ⓘ

Valid Mappings (37/42) Blank Mappings (5/42) Invalid Mappings (0/42)

Blank Source Applications	Mapping Mode	Target Application/Ports
panorama	Application	HTTPS
ms-ds-smb	Application	smb
ms-ds-smb-base	Select	NetBIOS-ssn (SMB)
ms-kms	Select	SMB over QUIC
smtps	Select	SMBv1
		SMBv2
		SMBv3-encrypted
		SMBv3-unencrypted

Manual mapping for apps that are not auto-mapped



Complete list of applications is available at <https://appid.cisco.com/>

Optimize, Review & Validate

Migration Progress/Stage



Optimize, Review and Validate Configuration ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: FTD-2-Instance-1

Access Control Objects NAT Interfaces Routes Site-to-Site VPN ⓘ Remote Access VPN

☒ Select all 260 entries Selected: 260 / 260 Actions ▾ Save

⬇

✓	#	Name	SOURCE			DESTINATION			Application	URLs	State	Action	TIME BASED Objects
			Zone	Network	Port	Zone	Network	Port					
☒		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
☒	1		ANY		ANY	ANY		Ping	ANY	NA	✓	Allow	None
☒	2		ANY		ANY	ANY		ANY	syslog	NA	✓	Allow	None
☒	3		ANY		ANY	ANY		SYSLOG_PR...	ANY	NA	✓	Allow	None
☒	4		ANY		ANY	ANY		ANY	SSH, SNMP	NA	✓	Allow	None
☒	5		ANY		ANY	ANY		ANY	SNMP	NA	✓	Allow	None
☒	6		ANY		ANY	ANY		ANY	Netflow	NA	✓	Allow	None
☒	7		ANY		ANY	ANY		ANY	NTP, DNS	NA	✓	Allow	None
☒	8		ANY		ANY	ANY		NETBKP_AP...	ANY	NA	✓	Allow	None
☒	9		ANY		ANY	ANY		ANY	Microsoft System C...	NA	✓	Allow	None
☒	10		ANY		ANY	ANY		SCCM_PRIV...	ANY	NA	✓	Allow	None

Analysis

Process to optimize ACLs depends on factors like number of ACLs, number of objects referenced, size of the config, etc.

Estimated time to complete optimization is **3 min(s)**.

Click on **Proceed** to continue, else click on **Cancel**.

Proceed

Cancel

Recommendation - Please allow optimization to complete, else it will result in migration failures (Refer **Estimated time** above to confirm your next step).



Overview: ACL Analysis

Total ACL rules - 260

- Disabled ACL rules - 3

ACL rules considered for optimization - 257

- Redundant ACL rules - 0
- Shadowed ACL rules - 96
- Unique ACL rules - 161

Note - Some ACLs may overlay between redundant and shadow rules, refer detailed excel reporting available under ACL optimization section.

Click on **Yes** to proceed ahead with ACL optimization.

(New Interface will provide the ability to Review, Select and Optimize the original ACL rules)

Yes

No

Summary

Validation Status

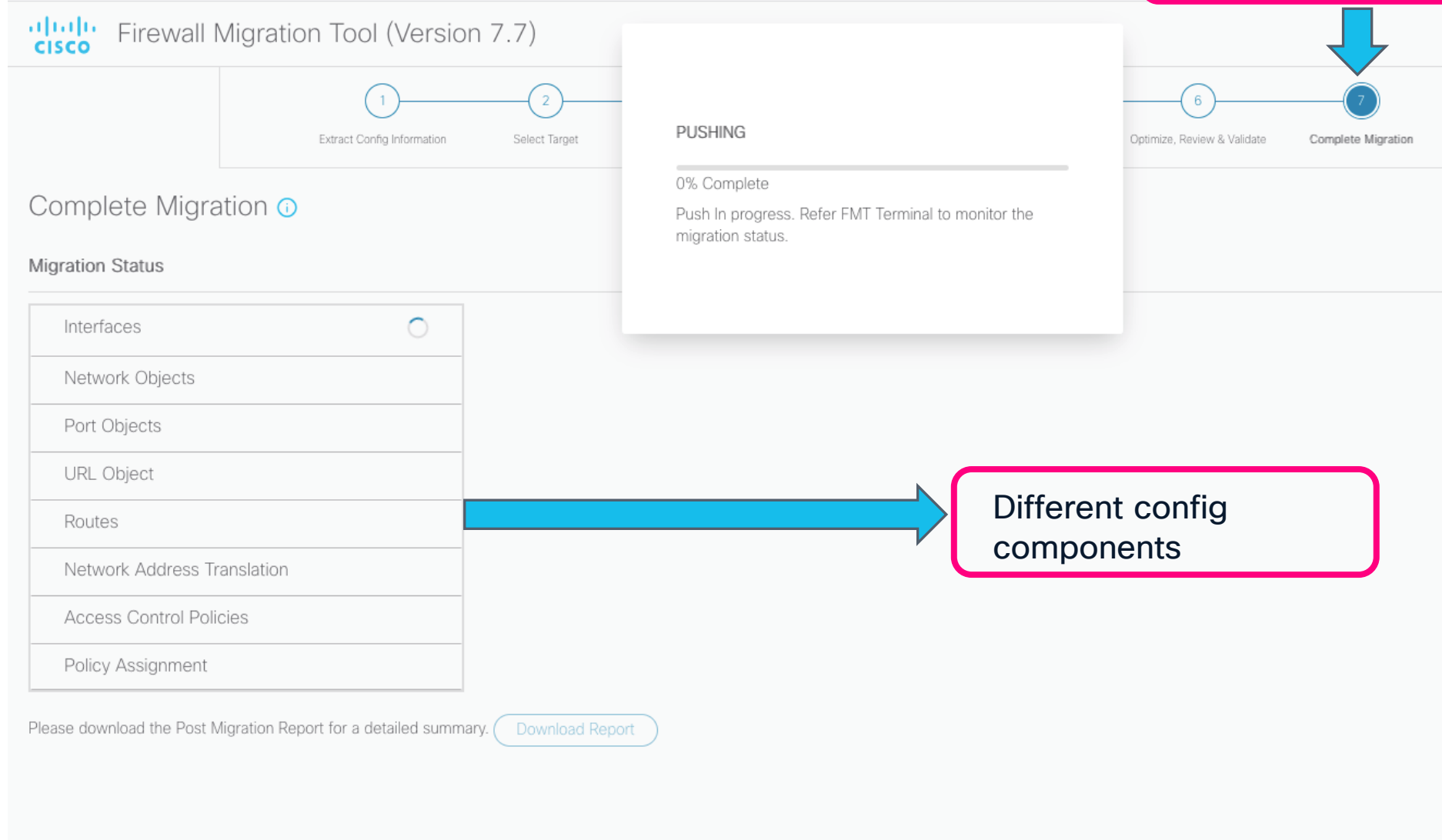


Successfully Validated

Validation Summary (Pre-push)

164 Access Control List Lines	1342 Network Objects	296 Port Objects	4 Network Address Translation	23 Logical Interfaces
30 Static Routes	Not selected for migration Site-to-Site VPN Tunnels	42 Applications	0 Remote Access VPN (Global Protect Gateways)	

Config Push



Configure sleep settings to prevent FMT failures during large configuration migration

Post-Migration Report

Migration Summary

- Configuration that are successfully migrated.
- Useful to compare with pre-migration report for differences.

Selective Policy Migration

- Details of feature selected for migrations

Migration Conversions

- Network/Service object handling
- Partially migrated & Unsupported configurations with reasons
- Expanded Access Control Rules

Validations

Static & Dynamic Validations

Static Checks

- Packet tracer
- Policy Analyzer Optimizer
- Best Practice Recommendations
- System Health
- Baseline

Dynamic Checks

- Elephant Flow Detection
- Configured Traffic Blocks
- System Health
- Application Performance
- Baseline



- Update any static routes which refer to the IP address (If IP address scheme is changed)
- For dynamic routing protocols, ensure that neighbors see FTD IP as the next hop for expected destinations
- Clear the Address Resolution Protocol (ARP) cache on the surrounding switching infrastructure

Firepower Device Migration

What's Shipping



FMC 7.4.0

Source

- 11XX: 1120, 1140 & 1150
- 21XX: 2110, 2120, 2130 & 2140

Target

- 31XX: 3105, 3110, 3120, 3130 & 3140

FMC 7.6.1

New Source

- 41XX: 4110, 4120, 4140 & 4150 (M4 Blades)
- 93XX: SM24, SM36 & SM44 (M4 Blades)

Target

- New 42XX Series: 4215, 4225 & 4245

FMC 10.0.0

New Source

- 41XX Series: 4112, 4115, 4125 & 4145 (M5 Blades)
- 9300 Series: SM40, SM48 & SM56 (M5 Blades)
- 1010 Series

Target

- New 12XX Series: 1210CE, 1210CP & 1210CX
- New 61XX Series: 6160 & 6170
- New 220 Series



All the source and target devices are forward compatible

Before We Begin

- Registered to same FMC(domain)
- No active tasks (Deployments, domain movement, import/export)
- Change the IP addresses of the interfaces if the source device is live, as they are copied to the target device from the source device.
- Update NAT policies with the modified IP addresses.
- Re-enroll the device certificates, if any, on the target device.
- Configure HA parameters such as monitored interfaces, failover trigger criteria, and interface MAC addresses.
- Configure the diagnostic interface as it gets reset after migration.
- Configure SNMP using the platform settings for the device.

Getting Started

CISCO

Firewall Management Center

Devices / Device Management

Q Search

Deploy

10

admin

Home

Overview

Analysis

Policies

Devices

Objects

Integration

View By: Group

All (19)

Error (1)

Warning (1)

Offline (14)

Normal (3)

Deployment Pending (5)

Upgrade (0)

Snort 3 (16)

Collapse All

Download Device List Report

☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
☐	Ungrouped (19)						
☐	<div><div>✓</div><div>10.10.29.14</div><div>Snort 3</div><div>10.10.29.14 - Routed</div></div>	Firewall Threat Defense for VMware	7.6.1	N/A	Essentials	None	<div><div></div><div></div></div>
☐	<div><div>✓</div><div>10.10.29.26</div><div>Snort 3</div><div>10.10.29.26 - Routed</div></div>	Firewall Threat Defense for VMware	7.7.0	N/A	Essentials	None	<div><div></div><div></div></div>
☐	<div><div>⚠</div><div>10.10.29.6</div><div>Snort 3</div><div>10.10.29.6 - Routed</div></div>	Firewall Threat Defense for VMware	7.7.0	N/A	Essentials	None	<div><div></div><div></div></div>
☐	<div><div>⌛</div><div>10.10.43.19</div><div>Snort 3</div><div>10.10.43.19 - Routed</div></div>	Firewall Threat Defense for VMware	7.7.0	N/A	Essentials	acp01	<div><div></div><div></div></div>

Migrate

Search Device

Add

Device Selection

1 Select source and target devices

Source device

Device name:

192.168.0.125 (Routed)

Device model: Cisco Firepower 4125 Threat Defense

Device version: 7.6.1

Mode of the device should be identical on Source and Target

Target device

Device name:

3105 (Routed)

Device model: Cisco Secure Firewall 3105 Threat Defense

Device version: 7.6.1

Target Device Version must be same or higher than Source Device Version



Forward Error Correction is available on 25G/100G interfaces on 31XX/42XX platforms

Chassis Manager Details

2 Chassis manager details

☐ Skip chassis manager

Hostname or IP address ⓘ

Username

Password

Verify certificate

✓ Certificate verified

Certificate

Issued to

Common name CL-FTD

Organization

Organization unit

Issued by

Common name CL-FTD

Organization

Organization unit

Serial number

Validity period

Issued on Wednesday 12 September 2018 at 09:49:10

Expires on Saturday 9 September 2028 at 09:49:10

SHA-256 fingerprint

Certificate

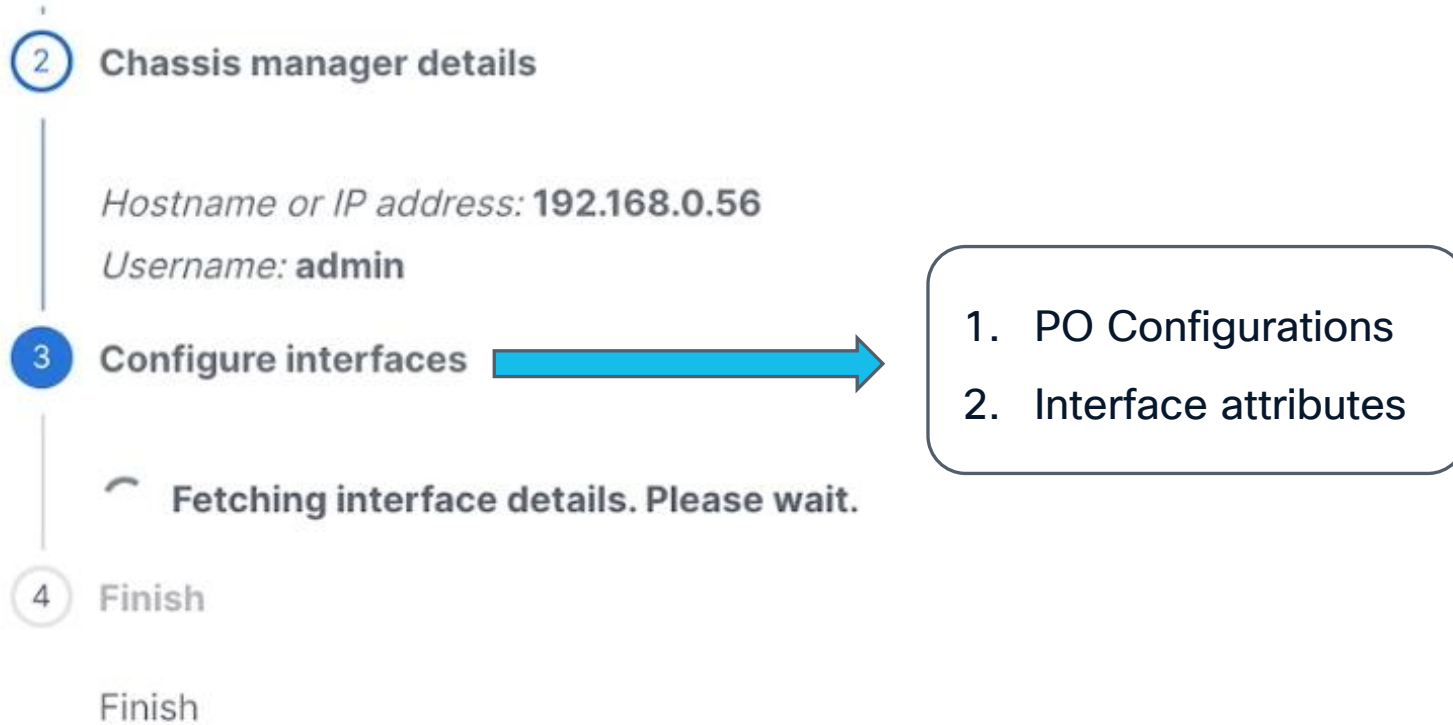
Public key

OK



This step is applicable for 4100/9300 devices to extract config done from chassis manager

Chassis Manager Details



Interface Mapping

3

Configure interfaces

Map source device interfaces to the target device interfaces.

Interface attributes

Click one of the radio buttons to configure the speed, duplex, autonegotiation, and FEC interface attributes.

1

☒ Retain target device values

2

☐ Copy from source device

3

☐ Customize device values

Interface

Name

Speed

Duplex

Mapped interface

Media

Speed

Duplex

Autonegotiation

FEC mode

Port-channel2		10 Gbps	Full	Port-channel2		<div>Speed</div> <div></div>	<div>Duplex</div> <div>10</div> <div></div>	<div>Autoneg</div> <div></div> <div></div>	<div>Add member interface</div>
Ethernet1/2				<div>Choose an interface</div> <div></div>					<div>FEC mode</div> <div></div> <div></div>
Ethernet1/4	eth4	10 Gbps	Full	<div>Choose an interface</div> <div></div>		<div>Speed</div> <div></div>	<div>Duplex</div> <div>10</div> <div></div>	<div>Autoneg</div> <div></div> <div></div>	<div>FEC mode</div> <div></div> <div></div>
Ethernet1/7		10 Gbps	Full	<div>Choose an interface</div> <div></div>		<div>Speed</div> <div></div>	<div>Duplex</div> <div>10</div> <div></div>	<div>Autoneg</div> <div></div> <div></div>	<div>FEC mode</div> <div></div> <div></div>

☐ Ignore warnings

Previous

Next

Reset

- 1

Interface Attributes from the Target Device are retained. Default Option
- 2

Interface Attributes are copied from Source to Target Device
- 3

Interface Attributes are customized from their default settings



Speed, duplex, and auto negotiation values are set to default if copied values are incompatible

Interface Mapping Summary

3 Configure interfaces

Interface attributes: User-provided values

Interface	Name	Speed	Duplex	Mapped interface	Media	Speed	Duplex	Autonegotiation	FEC mode
Port-channel2		10 Gbps	Full	Port-channel2		10 Gbps	Full	False	
Ethernet1/2				Ethernet1/6	SFP				auto
Ethernet1/4	eth4	10 Gbps	Full	Ethernet1/4	SFP	10 Gbps	Full	False	auto
Ethernet1/7		10 Gbps	Full	Ethernet1/7	SFP	10 Gbps	Full	False	auto

4 Finish

[Previous](#)

[Submit](#)



Only Data interfaces are listed for interface mapping

Migrate

1. Post reviewing the interface summary. Proceed with “Submit”
2. Click “Submit” to initiate the migration task
3. Progress can be monitored through task notification
4. Once completed, user is notified along with “Download Report” option

Migration initiated successfully. Progress is displayed under the **Tasks** tab.

OK

Dismiss all notifications



Device Model Migration

Device model migration complete for CL-FTD

[Download Report](#)



The device will not be automatically deployed as part of the process; it will just be configured

FMC Migration

On-Prem Model Migration

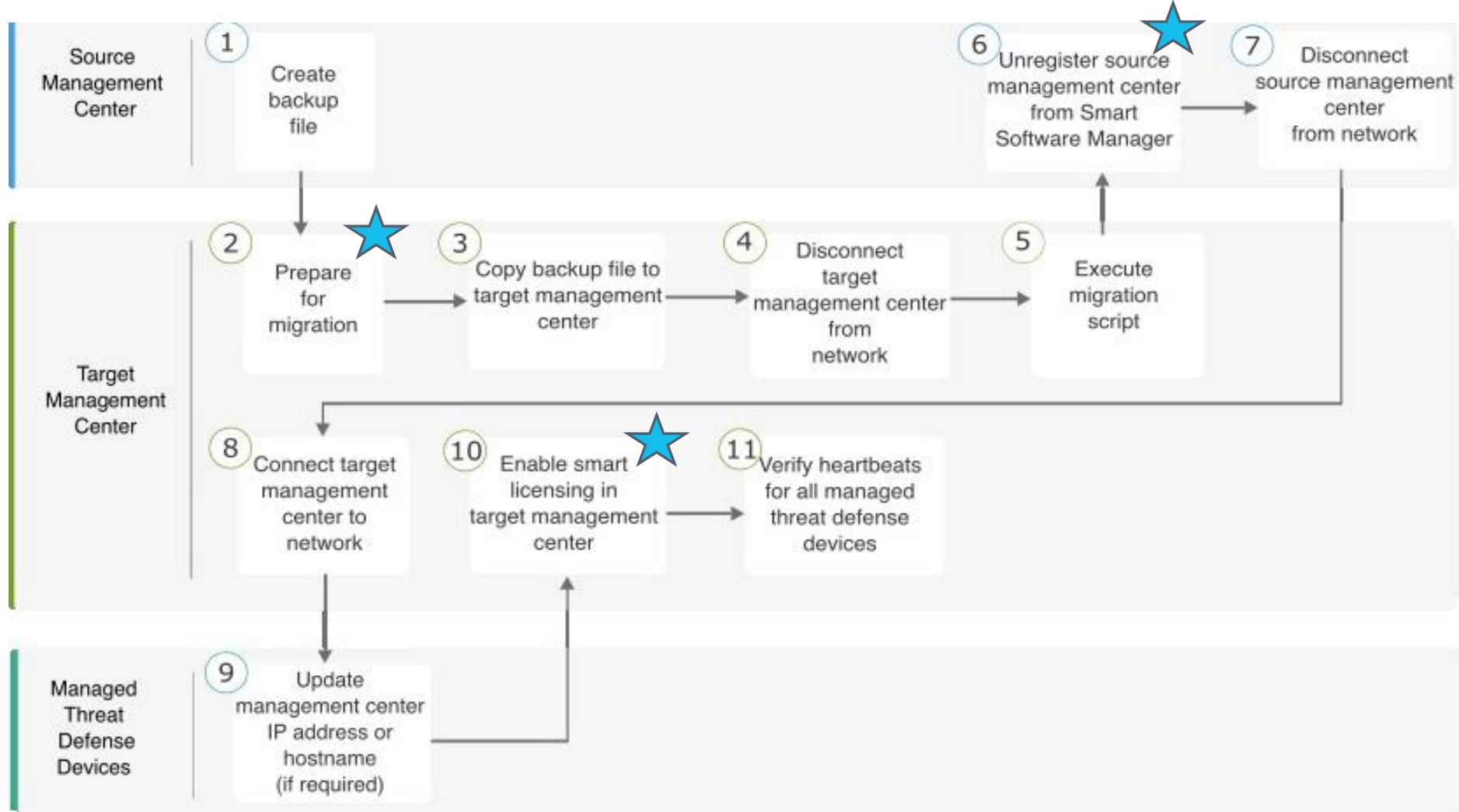
Prepare for Migration

- Target FMC should not have managed devices
- Target FMC should not be a part of High availability
- FTD registration, Deployment, & Backup should not be running during migration
- Supported migration path from the source to target FMC
- Classic license is not available for FMC Version 7.6+, as NGIPS is not supported
- Backup Availability



Model Migration Path: [Supported Paths](#)

Migration Workflow (Pre 10.0.0)



Before model migration, you must delete existing classic licenses.

Migration Script

- Log in to the target management center CLI.
- Run the expert command to switch to expert mode.
- Execute the migration command:

`/var/sf/bin/sf-migration.pl backup_file_path`

- Example:

`root@firepower:# /var/sf/bin/sf-migration.pl /var/sf/backup/source_local_backup`

Post Migration Activities

- From Version 7.4.x, update the following parameters, as needed:
 - IP address of the target FMC.
 - If the IP address of the FMC changes, edit the FMC Address in the threat defense devices.
*This is not required if the management center can reach the threat defense device.
- Licensing
 - Smart Licensing: Deregister the licenses from the source FMC and register the licenses in the target FMC.
 - Classic license: Contact TAC to regenerate the license using the new MAC address of the FMC.



- After migration, if you want to manage a different group of FTD in the source FMC:
- Ensure that source FMC cannot reach the stale FTD.
- Delete the stale FTD that are now managed by the target FMC

Migrating to Public Cloud

- Use reserved static public IP addresses instead of default public IP addresses.
- Use FQDN/DNS name because it can be moved across the public IP addresses.
- If you do not want to update the public IP address of the target management center virtual, run the following command in the threat defense device CLI:

configure manager add DONTRESOLVE any_key any_key_for_nat_field_input

- Before you run the above command, ensure that the management center virtual can connect to the threat defense device.
- If you do not perform the above operations, you must update the management center virtual IP address on the threat defense device using the following command in the threat defense device CLI:

configure manager edit fmc_uuid displayname fmc_ipaddress

TAC Insights

Category	Error Message	Remediation
Hardware/Software	<ol style="list-style-type: none">1. No migration path exists2. Interface count mismatch3. Migration data size is greater than the storage space of the target management center4. Software version, SRU, LSP and VDB mismatch	<ol style="list-style-type: none">1. Migration path not supported2. Source & Target should have same number of interface3. Increase the size of target management center4. Ensure software conformance
<i>Licenses</i>	<ol style="list-style-type: none">1. Device count is more than XXX2. Out of compliance3. Unable to communicate to licensing server	<ol style="list-style-type: none">1. Licenses for managed device is less.2. Insufficient licenses/unable to connect to licensing server3. Connectivity issue (Proxy connection)
<i>Connectivity</i>	<ol style="list-style-type: none">1. Devices not registered after migration2. Devices show disabled on FMC3. Policy Deploy failures	<ol style="list-style-type: none">1. Check port requirements on 83052. IP and Port connectivity from target FMC3. SFTunnel connectivity (8305)
<i>Backup/Restore Failures</i>	<ol style="list-style-type: none">1. Database corruption2. Version mismatch	<ol style="list-style-type: none">1. Reach out to TAC for assistance2. Software Conformance

New Migration Workflow (10.0.0)

The screenshot shows the Cisco Firewall Management Center (FMC) dashboard. The left sidebar contains a menu with the following items: Administration, Insights & Reports, Events & Logs, Policies, Objects, Firewall Devices, Secure Connections, Troubleshooting, and Administration. The 'Insights & Reports' menu item is highlighted with an orange box, and a blue arrow points from it to a text box that reads 'Option Available under Insights & Reports'. The 'Migrate Management Center' option is also highlighted with an orange box, and a blue arrow points from it to a text box that reads 'Option to migrate the Management Center'.

Option Available under Insights & Reports

Option to migrate the Management Center

The dashboard displays the following sections:

- Administration**: Configuration, High Availability, Users, Domains, Alerts, Upgrades & updates (Product Upgrades, Content Updates), Licenses (Smart Licenses), Advanced (Migrate Management Center, Backup & Restore, Scheduling, Import & Export).
- Insights & Reports**: Configuration, High Availability, Users, Domains, Alerts, Upgrades & updates, Licenses, Advanced.
- Events & Logs**: Intrusion Events, Status, Shadow Traffic, Geolocation, QoS.
- Policies**: Policies, Objects, Firewall Devices, Secure Connections.
- Troubleshooting**: Troubleshooting, Administration.

Top Web Applications Seen

Application	Total Bytes (KB)
HTTP Tunnel	1,064,064.05
SOAP	23,582.86
Docker	13,852.92
CDN77	12,562.66
Ubuntu Update Manager	10,820.67
Ubuntu	5,935.52
GNOME	3,188.65
Zimbra	378.44
Microsoft	11.05
Microsoft NCSI	11.05
Google	8.69
Paessler PRTG Network Monitor	0.78
imo.im	0.63
Cisco	0.23

Last updated less than a minute ago

Top Server Applications Seen

Application	Total Bytes (KB)
HTTP Tunnel	1,220,321.42
SOAP	1,216,438.56
Docker	1,091,603.8
CDN77	27,527.75

New Migration Workflow (10.0.0)

Secure Firewall Management Center Migration

1 Choose migration method

2 Prepare & start migration

3 View migration status

Choose migration method

Secure Firewall Management Center allows you to migrate from one management center model to another management center model.

The primary migration method is by connecting to the source management center. Alternatively, you can upload a migration bundle.

For prerequisites, supported migration paths, and so on, see [Online Help](#)

Connect to source management center

Source Firewall Management Center IP address

eg. 192.168.1.1

Username

eg. admin

Password

Connect

Live Connect to Source FMC
(Connected Mode)

Upload migration bundle

Upload Backup

Bundle Mode

New Migration Workflow (10.0.0)

Secure Firewall Management Center Migration

1 Choose migration method

2 Prepare & start migration

3 View migration status

Prepare and start migration

Source Firewall Management Center

Previous

Model	Cisco Secure Firewall Management Center for VMWare
Version	7.6.0
Managed device count	1
Device limit	25
Snort rule update	2025-04-02-001-vrt
Vulnerability database	build 405
Lightweight security package	lsp-rel-20250305-2047
Geolocation	2025-03-20-088
High availability status	Secondary Active Degraded

Target Firewall Management Center

Current

Model	Cisco Secure Firewall Management Center for VMWare 300
Version	10.0.0
Managed device count	0
Device limit	300
Snort rule update	2025-04-02-001-vrt
Vulnerability database	build 405
Lightweight security package	lsp-rel-20250305-2047
Geolocation	2025-04-03-094
High availability status	Standalone

☐ Migrate events

If events are needed

Compatibility check

Retry

Compatibility check identified the following warnings. Review and proceed.

- Geolocation version mismatch, Source Geolocation version is 2025-03-20-088 and target Geolocation version is 2025-04-03-094.

Cancel

Start migration

Hardware & Software Details

If events are needed

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2058

 CISCO

New Migration Workflow (10.0.0)

Secure Firewall Management Center Migration

1 Choose migration method

2 Prepare & start migration

3 View migration status

Prepare and start migration

Source Firewall Management Center

Previous

Model	Cisco Secure Firewall Management Center for VMware
Version	7.8.0
Managed device count	1
Device limit	25
Snort rule update	2025-04-02-001-vrt
Vulnerability database	build 405
Lightweight security package	lsp-rel-20250305-2047
Geolocation	2025-03-20-088
High availability status	Primary Active

→

Target Firewall Management Center

Current

Model	Cisco Secure Firewall Management Center for VMWare 300
Version	7.8.0
Managed device count	0
Device limit	300
Snort rule update	2025-04-02-001-vrt
Vulnerability database	build 405
Lightweight security package	lsp-rel-20250305-2047
Geolocation	2025-03-20-088
High availability status	Standalone

☐ Migrate events ⓘ

Compatibility check

Retry

✔

 Compatibility check successful. Proceed to migrate.

< Cancel

Start migration

New Migration Workflow (10.0.0)

Secure Firewall Management Center Migration

1 Choose migration method

2 Prepare & start migration

3 View migration status

View migration status

✓ Firewall Management Center migration initiated successfully.

○ Migration initiation on source management center
Updated 1 second ago
Running pre-migration validations

○ Migration bundle generation

○ Migration bundle transfer

○ Migration initiation on target management center

Phases of migration

Last updated: 1 second ago

[Cancel](#)

New Migration Workflow (10.0.0)

Source Management Center Hostname: **firepower-src1**
Target Management Center Hostname: **firepower**

100 % 

 **Migration has completed. Please click the reboot button.**

Before clicking reboot unregister Licenses and shutdown the source FMC. Register licence in this setup post reboot.

New Migration Workflow (10.0.0)

```
root@firepower:/etc/rc.d/modelmigrationboot.d# fmc_model_migration_cli.pl
```

```
***** Management Center Model Migration *****
```

```
This Management Center information:
```

```
Management Center Version : 10.0.0
```

```
Model : Cisco Secure Firewall Management Center for VMWare 300
```

```
UUID : 71df26dc-5c8a-11f0-9b2a-2c63491baa60
```

```
Managed devices limit : 300
```

```
*****
```

```
No TGZ file path provided, using default: /etc/rc.d/modelmigrationboot.d/modelmigrationboot.d.tar.gz
```

```
Extracting /etc/rc.d/modelmigrationboot.d/modelmigrationboot.d.tar.gz to /var/tmp/fmc-migration...
```

```
Do you want to migrate events? (yes/no): yes
```

```
Configuration and events will be migrated.
```

```
Do you want to proceed with the migration? (yes/no): yes
```

```
Starting migration script...
```

```
Migration process started with PID: 32470
```

```
You can monitor the progress with /var/log/fmc_migration.log
```

```
root@firepower:/etc/rc.d/modelmigrationboot.d#
```

Execute the command at the CLISH
`sudo fmc_model_migration_cli.pl`

Notice that Do you want to proceed with migration answer is “yes”. This starts the operation.

New Migration Workflow (10.0.0)

Secure Firewall Management Center Migration

1 Choose migration method

2 Prepare & start migration

3 View migration status

Choose migration method

Secure Firewall Management Center allows you to migrate from one management center model to another management center model.
The primary migration method is by connecting to the source management center. Alternatively, you can upload a migration bundle.
For prerequisites, supported migration paths, and so on, see [Online Help](#)

Connect to source management center ?

Source Firewall Management Center IP address

Username

Password

Connect

Cancel

Upload migration bundle

New Migration Workflow (10.0.0)

Secure Firewall Management Center Migration

1 Choose migration method

2 Prepare & start migration

3 View migration status

Choose migration method

Secure Firewall Management Center allows you to migrate from one management center model to another management center model. The primary migration method is by connecting to the source management center. Alternatively, you can upload a migration bundle. For prerequisites, supported migration paths, and so on, see [Online Help](#)

Upload migration bundle

1. Create a migration bundle. See [online help](#) for instructions.

2. Upload the migration bundle.

source_database_content_fmc1.t...

0.26 / 0.345 GB

Cancel

Uploading

Connect

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2058

 CISCO

New Migration Workflow (10.0.0)

Secure Firewall Management Center Migration

1 Choose migration method

2 Prepare & start migration

3 View migration status

View migration status

✓ Firewall Management Center migration initiated successfully.

● Migration initiation on source management center

Skipped

● Migration bundle generation

Skipped

● Migration bundle transfer

Skipped

○ Migration initiation on target management center

Updated 1 second ago

Running pre-migration validations: 1

<

Cancel

New Migration Workflow (10.0.0)

FMC HA Model Migration Workflow Overview

- A pair of source FMCs in HA and two standalone target FMCs.



- Overview of Steps
 1. Migrate the Active source FMC Primary to one of the standalone target FMCs.
 2. Deregister Active source FMC Primary from Smart Licensing and shut it down.
 3. Migrate the Standby source FMC secondary to the other standalone target FMC.
 4. Deregister Standby source FMC Secondary from Smart Licensing and shut it down.
 5. Resolve split-brain between the two targets.

Migrating FTD to cdFMC

Prepare for Migration

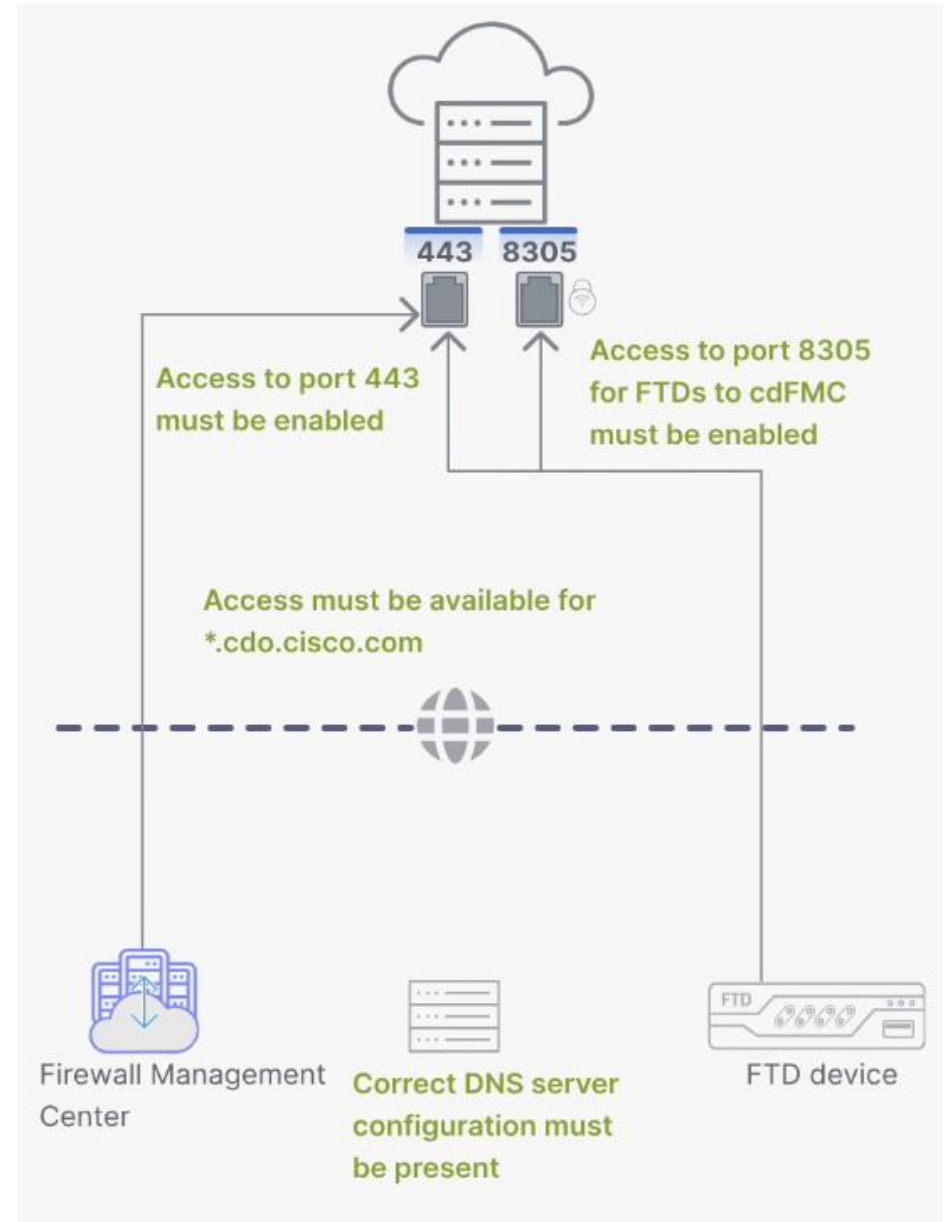
- Upgrade the on-premises FMC/FTD to a SCC-supported version
- Onboard the FMC to SCC
- We support a temporary upgrade from 7.0 to 7.4 (FMC:1000/2500/4500)
- Ensure you have registered the cdFMC with a smart license
- Check for supported features

Points to remember

- If a policy in cdFMC shares the same name as one in On-Prem FMC (excluding network, port, URL, and VLAN objects), the cdFMC version will be retained
- After migration, policies and objects aren't auto-synced. For phased migrations, you must update them manually.
- You can revert to On-Prem FMC within 14 days of migration. After that, changes are finalized automatically.



Additional Info



Migration Process (1/3)

Migrate FTD to cdFMC

Migrate FTD to cdFMC

Migrate FTD from On-Prem FMC to cloud

Cancel

1 Before you begin

2 Select On-Prem FMC

1 Ensure that you have onboarded your On-Prem FMC to SCC using the [Auto discover from Cisco Security Cloud](#) method or the [Use Credentials](#) method. See [Onboarding On-Prem FMCs](#).

2 After your On-Prem FMC has been onboarded, select it from the list.

Available On-Prem FMCs (7.2+ only)

Select On-Prem FMC

cisco_live_fmc_1

cisco_live_fmc_2

cisco_live_fmc_3

cisco_live_fmc_4

3 Select Devices

4 Finish

Migration Process (2/3)

Migrate FTD to cdFMC

2

Select On-Prem FMC

On-Prem FMC: firepower_10.10.12.2 10.10.12.2

3

Select Devices

Select FTD device(s) to migrate from On-Prem FMC to cloud, and specify an action in bulk or per device.

Last Synced time : 2 minutes ago Sync from On-Prem FMC now

Q

Name

Multi-Device Action

Retain on OnPrem FMC for Analytics

☐	Name	Domain	Commit Action
☐	lvi_ftd_ha	Global	Retain on OnPrem FMC

0 device(s) selected

Displaying 1 of 2 results

Your On-Prem FMC is registered to a valid Smart License, but the cloud-delivered FMC license is in evaluation mode. This may degrade the security levels of policies after migration. To retain the security levels, register the cloud-delivered FMC with a Smart License or click 'Migrate FTD to cdFMC' to proceed with the migration.

☐ Pause migration to review imported shared policy

☐ Auto deploy to FTDs after successful migration

1

Ensure that the DNS and other required configurations are correct for the selected FTD(s) to reach SCC. Learn more

1

It's possible to revert the device back to its previously-registered On-Prem FMC by migrating to the cloud-delivered FMC. After migration job is completed with the actions selected without requiring further action from you. Learn more

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2058

Migration Process (3/3)

Migrate FTD to cdFMC

<div><div><div></div><div>Search by Name, Device Name or IP Address</div></div><div>Displaying 1 of 1 results</div><div><div></div><div></div></div></div>				
Name	Number of FTDs	Status	Last Updated	Actions
<div><div></div><div>firepower_10.10.12.2_ftd-migration_2025-10-06</div></div>	1 devices	<div><div></div>Migrate FTD to cdFMC job is in progress</div>	Oct 6, 2025, 12:53:27 PM	<div><div></div></div>
DEVICE NAME	MIGRATION STATUS		COMMIT STATUS	LAST UPDATED
lvl_ftd_ha	<div><div></div>Fetching the latest device inform...</div>			Oct 6, 2025, 12:53:26 PM

TAC Insights

Error Reported	Cause	Remediation
<i>Configuration export from On-Premises Firewall Management Center failed</i>	<ol style="list-style-type: none">1. Disk space is full or nearly full.2. Concurrent operations such as device upgrade, upgrade revert, device import and export, or policy analysis are running in on-premises FMC.3. Connectivity issues exist between the on-premises FMC and SCC.	<ol style="list-style-type: none">1. Ensure that at least 10% of disk space is available to accommodate the creation of necessary export files.2. Ensure that no parallel operations are running during the migration.3. Ensure that the network connection between on-premises FMC and SCC is stable and reliable.
<i>Failed to commit migration; the device is ineligible</i>	<ol style="list-style-type: none">1. The device has pending changes that have to be deployed.2. The device to be migrated is part of FTD high availability (HA), but the current state is invalid, for example, it is in Active/Active state.3. The device to be migrated is connected in Analytics-only mode.4. Cluster migration is supported only for FTDs version 7.4 and above.5. Migration for chassis and MI FTDs on models 3100/4200 is currently not supported.	<ol style="list-style-type: none">1. Verify that the device is up to date with On-Premises FMC.2. Ensure all pending changes on the devices are deployed.3. Confirm that the Firewall Threat Defense device is in a valid state



More Insights

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: raghukul@cisco.com

Thank you

CISCO Live !